

Technology Collection Trends in the US Defense Industry



19981015 071

1998

DISTRIBUTION STATEMENT A

Approved for public release;
Distribution Unlimited

REPRODUCTION QUALITY NOTICE

This document is the best quality available. The copy furnished to DTIC contained pages that may have the following quality problems:

- **Pages smaller or larger than normal.**
- **Pages with background color or light colored printing.**
- **Pages with small type or poor printing; and or**
- **Pages with continuous tone material or color photographs.**

Due to various output media available these conditions may or may not cause poor legibility in the microfiche or hardcopy output you receive.



If this block is checked, the copy furnished to DTIC contained pages with color printing, that when reproduced in Black and White, may change detail of the original copy.

**TECHNOLOGY COLLECTION TRENDS
IN THE
US DEFENSE INDUSTRY**

Table of Contents

I. Introduction.....	2
II. Executive Summary.....	2
a. Technology Interest Trends.....	2
b. Country Trends.....	2
c. Most Frequently Reported Technology Targets for 1997.....	3
d. Most Frequently Reported Methods of Operation (MO) for 1997.....	4
III. Reporting Status.....	5
IV. Technology.....	6
a. Interest Trends.....	7
b. Foreign Interest in Most Sought Technology.....	8
V. Foreign Collection Methods (MO).....	13
VI. Technology MO Correlation.....	16
a. Trends.....	16
b. Technical Intelligence Collection.....	22
c. Sequential Use of MOs.....	22
VII. Assessment of Future Trends.....	24
a. Countries.....	24
b. Targets.....	24
c. MOs.....	25

I. Introduction

This study is a Defense Security Service (DSS) counterintelligence (CI) tool for security professionals. It is designed to help cleared companies and DSS personnel recognize and report suspicious foreign activity so DSS can assist cleared companies enact responsive, threat-appropriate, and cost-effective security countermeasures (SCM).

II. Executive Summary

a. **Technology Interest Trends:** The volume of suspicious activity reporting in 1997 helped DSS assess current trends and forecast future trends. Foreign interest was reported in all Militarily Critical Technology List (MCTL) categories in 1997. Section III describes foreign technology interests.

Foreign entities continue to target weapon components, developing technology, and technical information more intensely than complete weapons systems and military equipment. Foreign interests sometimes prefer older "off-the-shelf" hardware and software, and/or seek International Traffic of Arms Regulations (ITAR)-controlled technology that is at least a generation old. The apparent purposes for these activities are concealing military end use, reverse engineering older components, or modernizing national infrastructures or capabilities.

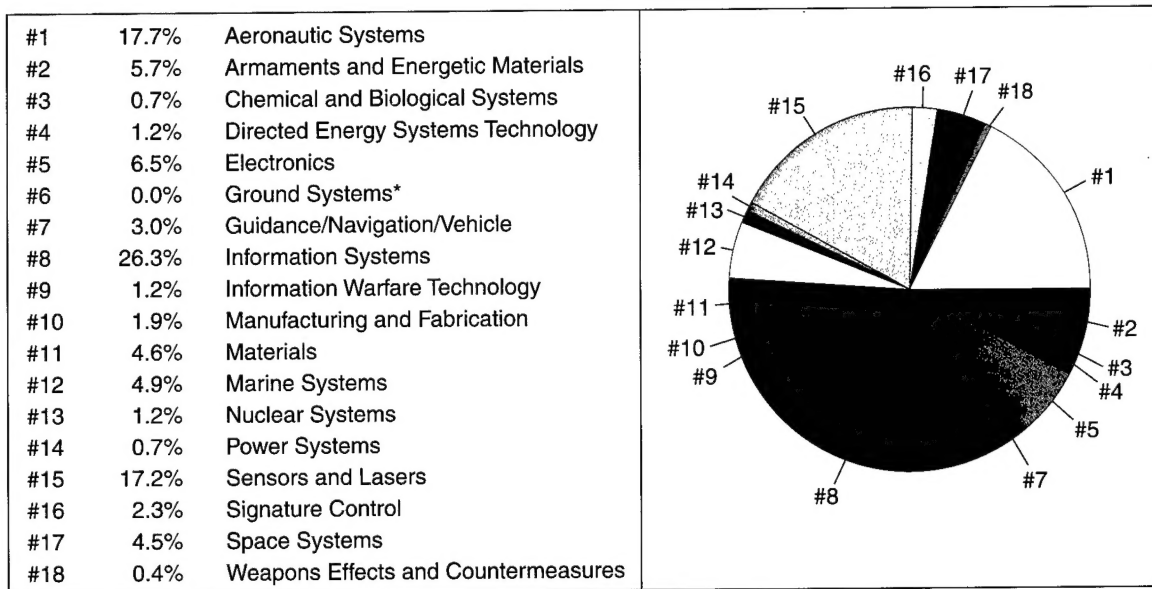
b. **Country Trends:** Reporting indicates less developed countries seek older technologies that cost less but still improve their military capability. More developed and traditional threat countries appear to seek technical information to kill, copy, counter, or cause significant change to US military systems. This has economic and battlefield implications. While nontraditional threats often seek US command, control, and decisionmaking equipment, plus major ground, airborne, and seaborne weapon systems information to enhance interoperability, this has potential economic disadvantages for US industry. Associated technology transfers and reverse engineering both cut into US defense industry markets. The number of countries seeking US technologies in 1997 was 37, to include all countries assessed as most and moderately active in 1995 and 1996. DSS forecasts countries assessed most and moderately active from 1995-97 will continue technology collection operations against the US defense industry.

c. **Most Frequently Reported Technology Targets:** Technologies generating most foreign interest this year were information systems, aeronautics, sensors, electronics, and armaments and energetic materials. This trend is somewhat consistent with business and military commander demands, a shift from information volume to efficiency. The Information Age has empowered public and private sectors with resources to define and describe conditions for decisionmakers: data handling systems provide total recall, high performance computers provide cost-benefit analysis or flexible manufacturing options in seconds, communication media convey facts rapidly. DoD leaders supplement these command, control, communication, and computer (C4) components with intelligent sensors to improve situation awareness, provide early warning of enemy activity, and increase combat efficiency — guiding weapons to targets. US infrared and electro-optic sensors can be applied to ground, airborne, and space systems and continue to generate foreign interest.

A common enabling technology for C4 and sensor technologies is the fourth most frequently targeted technology — electronics: materials and techniques that enable extreme density and high performance with low power. Large-scale integrated circuits, high-speed integrated circuits, and semiconductors have modernized US military capabilities and are found in virtually every US weapon system.

US aeronautics has generated foreign interest for many years. Current interest may be attributed to recent aerodynamics, engine designs, component integration, and digital electronics, enabling endurance and greater thrust ratios. Armaments and Energetic Materials, the fifth most frequently reported technology category, offers multiple means for applying the technology. With over 27 percent of the countries targeting this technology area, foreign interest is likely to continue.

Graphic #1, below, depicts the overall percentage of MCTL interest (listed alphabetically) reflected in the 1997 reporting.



Graphic #1

* The number of incidents involving Ground Systems were too few to graphically portray and usually involved supporting technologies generally related to other MCTL categories.

d. **Most Frequently Reported Methods of Operation (MO):** 1997 reports by cleared defense companies indicate several trends with respect to the variety of MO employed by foreign entities. MOs are the techniques employed by a foreign entity to collect against a given target. MOs associated with potential collection efforts in 1997 are as follows, ranked in order of frequency of occurrence:

- Unsolicited request for S&T information
- Inappropriate conduct during foreign visits
- Exploitation of joint ventures/research
- Targeting at international conventions and exhibits
- Solicitation and marketing of services
- Marketing surveys

- Acquisition of technology or company
- INTERNET
- Foreign employees
- Targeting of former company employees
- Targeting cultural commonalities

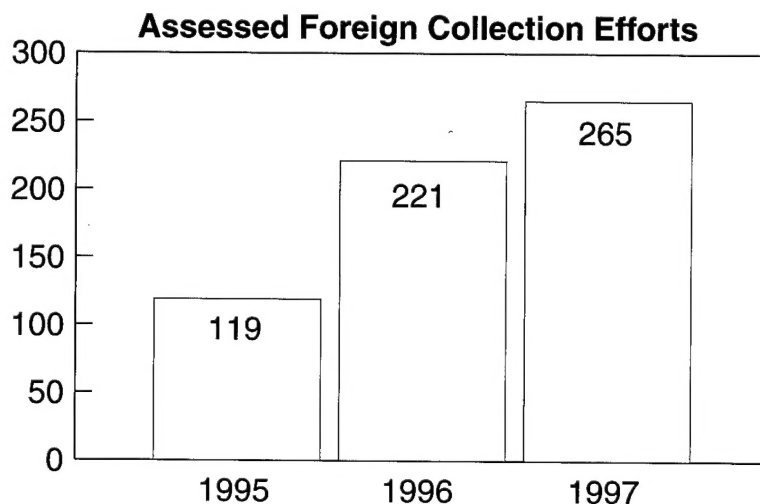
Unsolicited requests for information was the most frequently used collection method employed by foreign interests in 1997. While foreign interests employed a variety of methods, the methods are consistently similar to those reported in 1995 and 1996. Foreign collection methods and their frequency are described in Section V.

III. Reporting Status

Department of Defense (DoD) Directive 5240.2 requires DSS to assist industry in recognizing and reporting suspicious activity. Cleared companies and DSS responded well in 1997, increasing 1996 reporting volume by 41 percent. This continues a trend of increased awareness and reporting. These incident

reports continue to emphasize the importance of using company Facility Security Officers (FSOs) as a central coordination point for timely and comprehensive referrals of suspicious activity. Referrals conveyed to DSS at threat briefings or periodic reviews often limit DSS' capability because what may have been actionable was not forwarded to the FSO or DSS until months or years after the event.

Graphic #2 represents the number of reports, by year, of assessed foreign collection efforts.



Graphic #2

Overall reporting (both assessed collection efforts and suspicious contact reports) in 1996 more than doubled that of 1995, and 1997 reporting tripled that of 1995.

Whether for investigation or analysis, reporting helps educate industry, security, and CI professionals about foreign collection methods employed against US industry. **Thus, the CI Office needs to know, in greatest detail: the ultimate target (technology, system, or research), foreign identity (name and address), circumstances of the incident and background information (e.g., "met at convention in 1996"), and suspicious activity (e.g., "called a few times after I ignored his letter").** Timely reporting enables DSS immediately to deter and neutralize foreign collection activity at the lowest level.

Cleared company reporting indicates numerous successes in applying appropriate security countermeasures to potentially threatening situations. Many companies refused tours to unauthorized visitors, did not respond to suspicious foreign requests for information, refused inappropriate visit sponsorship requests, used effective escorts to control visiting delegations, and engaged authors of unsolicited e-mail to describe what they were interested in. This cordial entertainment of foreign requests proved useful in identifying and reporting inappropriate foreign interest. Most successes closely align with SCM outlined in the DSS brochure, **Suspicious Indicators and Security Countermeasures for Foreign Collection Activities Directed Against the US Defense Industry**, published May 1997. This indicates awareness training efforts in DSS and the defense industry have been effective.

IV. Technology

a. **Overview:** DSS documents and reviews foreign interest in US defense technology in categories described by the Militarily Critical Technology List (MCTL). The MCTL is the primary reference for DSS to identify and describe militarily critical technology. Sanctioned and published by DoD, it contains definitions of thresholds that make technology militarily critical.

A review of reported incidents of suspected targeting against critical technologies in 1997 has reaffirmed that every category of critical technology is subject to foreign interest for military and/or economic exploitation. Thirty-seven foreign nations were associated with suspected incidents of targeting. The extent of foreign interest in specific technology categories varies dramatically. Statistics discussed in this section are based solely on those technology categories that could be identified through incident analysis.

The vast majority of incidents demonstrated clear foreign targeting, intended use of information or technology, or a good identification of the foreign entity. Some reported

incidents involved peripheral technologies. Due to the breadth of technology application and the wide range of military and economic foreign interests, cleared companies are encouraged to provide detailed and specific reporting. These details will help DSS analysts determine foreign trends, intentions, and the ultimate target.

b. Technology Interest Trends. The most sought technology category was Information Systems (IS), which accounted for 26.3 percent of the total reported incidents where a technology category could be identified. Over half the 37 countries associated with suspected targeting of critical technologies in 1997 were identified as having targeted IS.

The 1997 IS targets included:

- Data fusion technology
- Information security systems
- TEMPEST/CRYPTO/COMSEC
 - KG-81 bulk encryption device
 - KG-84 data encryption device
 - CD-125 digital signal display
- Cluster computing technology
- Simulation and training systems
 - Photo realistic imaging in real time
- Telecommunications
 - Mobile telecommunications systems specifically emphasized
- Computers
 - Software and hardware designs
- Chaotic and adaptive signal processing
- Geographic information systems software.

In 1996 most suspicious IS foreign activity targeted the following, in descending order of occurrence:

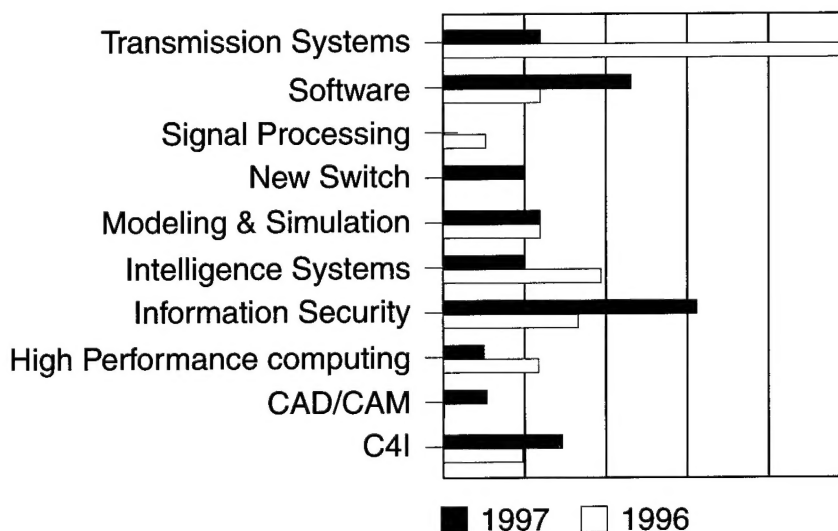
- Transmission systems, specifically radio and transmission components such as antennae, microwave absorbers, and telecommunications
- Intelligent computational systems (those providing algorithmic decision support)
- Information security
- Modeling & simulation, software, and high-performance computing (three-way tie)

In 1997, the majority of IS reports targeted enciphered and cryptographic information security for computer and communications networks. Software was next most frequent, then naval, ground, and air C4I systems.

Reports indicate a trend: 1996 foreign interest in IS primarily targeted advanced communicating and computing systems. 1997 reports indicate that the majority of foreign targeting concerned enabling and enhancing IS technology. Suspicious activities concerning information security (INFOSEC) and software subcategories and enhancements doubled from 1996, while C4I increased by 50 percent. Foreign interest in network and switching, an enabling technology, while not reported in 1996, was reported in 1997. Graphic #3 depicts these trends, identifying each MCTL subcomponent.

Many suspicious IS activities originated from countries the MCTL assessed as having no capability in IS subcategories. One country, assessed by the MCTL as having only limited network and switching technical abilities, requested such information. Another country, assessed as having no software or CAD/CAM capability, solicited software services to cleared companies and bid on contracts to write source code. This demonstrates how MCTL foreign technology assessments help assess foreign capabilities and probable intentions per reported incidents.

Information Systems
(Collection incidents per IS category per year)



Graphic #3

Aeronautics Systems and Sensors and Lasers were the second and third most targeted critical technology categories, accounting for 17.7 percent and 17.2 percent of the reporting, respectively. Just under 46 percent of the countries associated with targeting incidents went after Aeronautics Systems, while 41.6 percent of the countries targeted Sensors and Lasers.

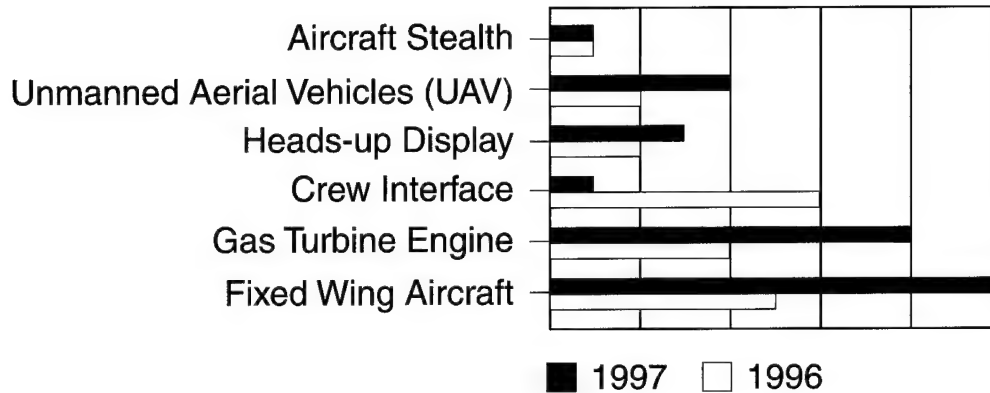
In the Aeronautics Systems category, identified targets included:

- Gas turbine engines
- Multi-band filter and power amplifiers for airborne applications
- UHF frequency agile filter-power amplifiers
- Aircraft electrical power distribution systems
- Frame relay switch routers
- Airborne laser mine detection
- Helicopters
- F-16A fighter
- AAQ-14 targeting pod testing
- Air-launched theater missile defense
- Unmanned aerial vehicles (UAV)
- Small turbojet engines
- Reliability growth testing
- Flight simulators
- Aircraft engine technology

Additionally, countries have targeted non-critical FAA collaborative decisionmaking system (CDS), weather forecasting computer (WFC) systems, and airport scheduling software. Exploitation of non-critical systems, such as the CDS, is valuable both commercially and as an exploitation means to reach restricted technology. WFC, for example, can modernize/improve commercial and military distribution of weather forecasts.

Foreign collection activity reports identify broader interest in US aeronautics from more countries. In 1996, advanced countries continued to target military and commercial aircrafts and engines, while being very interested in crew system interfaces, such as the helmet up display. In 1997, a greater number of developing countries targeted aircraft and engines, but did not appear interested in sophisticated enhancements. Overall interest level in aeronautics from 1996 and 1997 reporting is depicted in Graphic #4.

Aeronautics



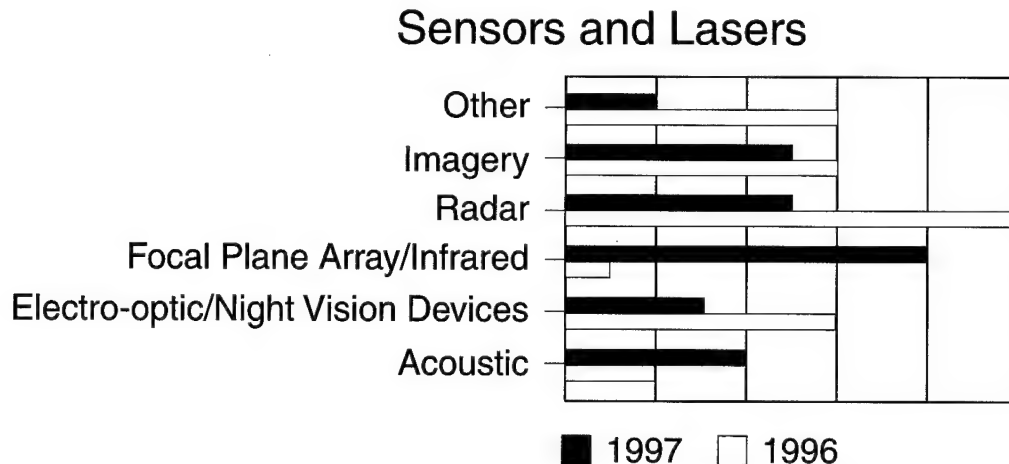
Graphic #4

In the Sensor and Laser category, reported foreign targets included:

- Refraction correction of vertical/ opaque imagery technology
- Gated intensified charge coupled device camera sensor systems
- Seaborne laser radars
- Electro-optical sensors
- Microwave imaging technology
- Wide-band inverse synthetic aperture radar systems
- APG-67 radar technology
- Pulse generator for the AN/APQ-130 attack radar (F-111D program)
- Infrared optical systems and lenses
- Surface acoustic wave technology
- Real-time sensor systems
- Ground-based phased array radars
- Data to construct object trajectory.

Focal plane array (FPA) and infrared (IR) radars were separated from the radar category to differentiate between strategic and tactical radars; however, some radar missions overlap. Foreign interest in radars that provide early warning to relatively small entities, such as aircraft and vessel, waned in 1997. Reports of foreign interest in IR technologies increased from 1996. Some foreign interests stated their intent to apply IR technology to commercial and environmental programs. These countries may have awaited documented success of commercial IR applications before seeking commercial applications, but, due to

the dual-use nature of airborne IR sensors, they can provide military information without modification.



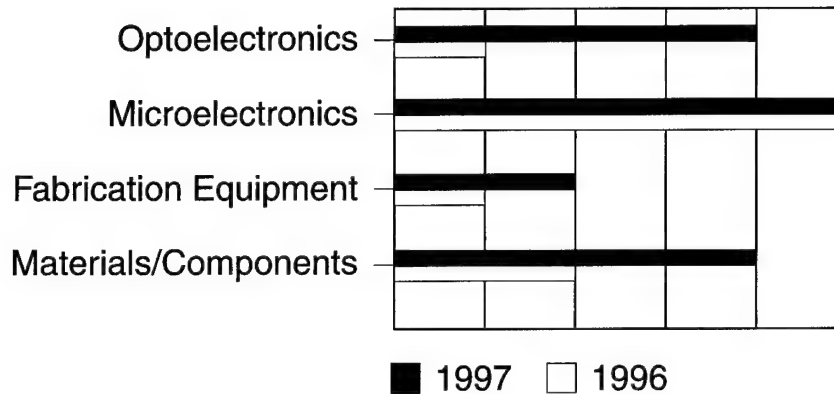
Graphic #5

FPA can be used in offensive (early warning) and defensive (countermeasure) situations. This may generate increased interest in 1998. The incident increase in 1997 is due, in part, to surface acoustic wave technology, which has both land-based and maritime applications. Relative interest levels between 1996 and 1997 reporting are depicted in Graphics #5.

Although attracting only 6.5 percent of the total targeting, approximately 20 percent of the 37 nations were involved in targeting Electronics. In Electronics, identified targets included:

- Reliability testing and test equipment
- Military applications of commercial electronics
 - Microwave components
- High technology and ruggedized components
- Earth and satellite antennae
- Electromagnetic (EM) and bio-EM technology and theory
- Pattern synthesis
- Nonlinear EM characteristics
- Inverse scattering and EM imaging
- Measurement techniques
- Traveling wave tube technology
- Electronic industrial controls

Electronics



Graphic #6

Armaments and Energetic Materials followed in fifth place, with 5.7 percent of the total number of incidents against identified technology categories. It should be noted that 27.7 percent of the 37 countries targeted this technology category. For this technology category there are multiple applications possible, thus identifying the specific targeted program was not always possible.

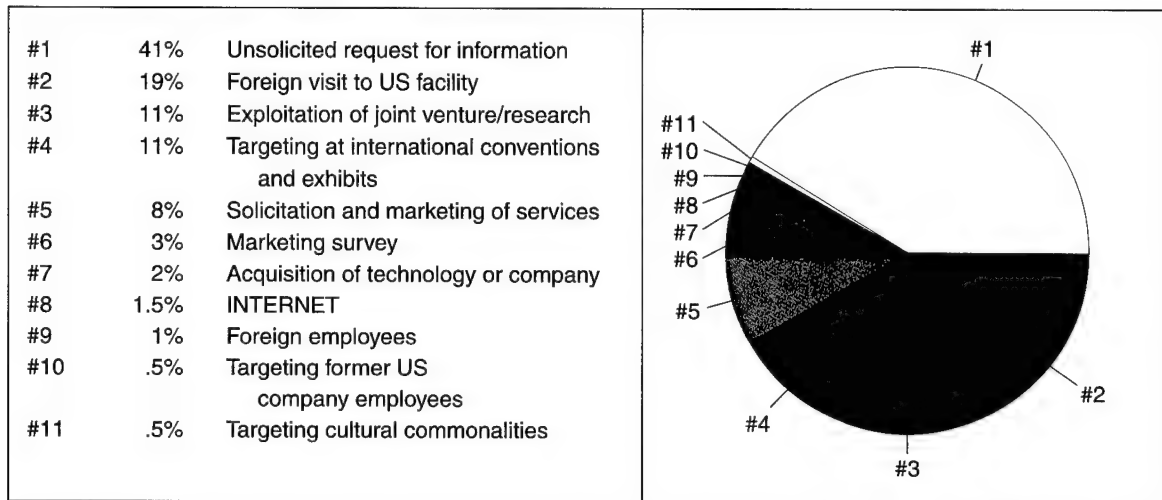
Rounding out the top eight technology categories identified in reported incidents were: Marine Systems at 4.9 percent, Materials at 4.6 percent, and Space Systems at 4.5 percent. In Marine Systems, identified targets were:

- Naval surface warfare systems
- Submarine-launched broadband acoustic jammers (counter-torpedo and sonar)
- Acoustical modeling for antisubmarine warfare
- Propulsion systems
 - Fluid self-propulsion phenomenon
 - Plasma and combustion augmented propulsion systems

Several countries were particularly interested in non-destructive material testing, including ultrasonic and X-ray tomography for composite materials. Foreign interest in Space Systems ranged from propulsion and vehicle control to infrared systems and earth horizon space sensors.

V. Foreign Collection Methods (MOs)

Graphic #7 depicts the frequency of each method of operation reflected in 1997 reporting. The numbers (#) correspond to the particular MO shown below. Note that MOs #3 and #4, as well as #10 and #11 respectively, were "tied" in the frequency of occurrence and were arbitrarily assigned their relative rankings.



Graphic #7

Unsolicited requests for US defense industry S&T program information is the most frequently reported MO associated with foreign collection activity. An unsolicited request for information is any request, not sought or encouraged by the cleared company, for information or business arrangement received from a known or unknown source. Since our office began keeping statistics in 1995, reporting of unsolicited requests for information has tripled. The requests have originated from foreign companies, individuals, government officials, and organizations and have been e-mailed, telephoned, faxed, and mailed. The INTERNET provides an anonymous method for making unsolicited requests.

In 1997, our office saw a resurgence in reporting unsolicited requests for information from restricted countries. Restricted countries are those that normally do not do business with the US or have embargoes placed on them. The factor that made the vast majority of these reports suspicious was the requirement that the information have a special license for export in accordance with the International Traffic in Arms Regulations (ITAR).

New twists to this MO are the "thesis request" and request for articles that have appeared in technical trade journals and periodicals. The "thesis request" is usually targeted at a specific individual at a cleared company. The "student" will state he/she is working on a thesis and located the US employee's name while conducting research. The student will ask for whatever help the cleared employee can supply, usually associated with a topic involving a technology covered by the ITAR or MCTL, or sometimes, a topic involving classified information.

Another variant of this MO is a request for a copy of a technical trade journal article from the article's author. The requester will occasionally ask detailed questions concerning the procedures or technical aspects relating to the article. Again, the topic normally falls under the MCTL or can be dual-use in nature.

Inappropriate conduct during **foreign visits** was the second most frequently reported MO. For the third year in a row foreign visits have continued to be frequently associated with suspicious activity. One factor that made many foreign visits suspicious was the extent to which the foreign visitor would request information outside the scope of what was approved for discussion. Suspicious indicators include:

- Inappropriate behavior
- Visitor presses for access and becomes irate upon denial of access or requested information
- Visitor wanders around the facility unescorted
- Individuals bringing cameras and/or video equipment into a cleared facility
- Hidden agenda associated with the stated purpose of the visit
- Last minute and/or unannounced persons added to the visiting group

A unique variation reported in 1997 was foreign nationals using approved visits to broker other visits to additional companies or subsidiaries on short notice. **Also being reported with more frequency are collection efforts by foreign personnel involved in multinational training.** Several incidents occurred when foreign nationals, during training, requested restricted and/or controlled technologies from their US counterparts. Even when initially denied the information, some foreign students made persistent further efforts to obtain the material. Inappropriate behavior during visits continues to be reported with more frequency. In recent cases involving foreign visits, individuals were observed bringing cameras and video equipment into cleared facilities. Some foreign visitors have attempted to take photographs of sensitive production lines.

Exploitation of Joint Venture/Research was the third most frequently reported MO. It offers significant collection opportunities for foreign interests. As with frequent foreign visits and other international programs, joint efforts place foreign personnel in close proximity to US personnel and afford potential access to S&T programs and information. A number of reports involved cleared personnel being targeted when traveling to foreign countries in order to perform work on joint ventures. Reporting indicates that possible front companies are using this MO. A front company works on behalf of a customer, often with the intent to hide the identity of the end user. Joint relationships are often associated with or lead to foreign acquisition of US technology.

International conventions, seminars, and exhibits are rich collection targeting opportunities for foreign collectors. These functions directly link programs and technologies with knowledgeable personnel. Corporate officials have reported possible telephone monitoring during international calls back to company headquarters. Several incidents reported hotel room intrusions — even when the room was still occupied! The technologies associated with these international conferences most often fall under dual-use. Increasingly, cleared companies are receiving invitations through the INTERNET to participate in conferences. Additionally, US technical experts are often asked by foreign entities to visit the foreign country and share their technical expertise in specific forums. While many requests are routine and benign, some are viewed with suspicion and represent an SCM concern. Audiences during these foreign seminars are often composed of leading scientists and technical experts within the country. These individuals can pose more of a threat than intelligence officers. The scientists focus their questions and requests on specific technical areas that have direct application to their research.

Reporting also shows that during seminars foreign entities may attempt more subtle approaches such as sitting next to a potential target and initiating a casual conversation. This can establish a point of contact that may be targeted later using other means (foreign visit, unsolicited request for information, etc.). Reporting has included incidents when foreign entities obviously knew a particular individual's travel arrangements and went as far as placing an agent next to the traveler while on commercial transportation.

Soliciting and marketing of services was the fifth most frequently reported MO. Consistent with past reporting, foreign individuals with technical backgrounds offer their services to research facilities, academic institutions, and even cleared defense companies. Some incidents involved foreign nationals seeking postdoctoral fellowships at cleared universities. **Emigres** are continuing to seek employment at companies involved in cutting-

edge technologies. **A new MO trend this year is foreign individuals who fabricate past work histories in an attempt to gain employment with cleared companies in unclassified positions. A variant of this MO was foreign software manufacturers soliciting products to cleared companies after embedding into the software spawned processes and multi-threaded tasks.** In several instances, precise specifications relating to the technologies the cleared companies were working on were requested by the foreign entity before providing their services.

Various types of **marketing surveys**, faxed or mailed to US companies by foreign consortiums or "consulting" companies, exceed generally accepted terms of marketing information. Often, there are strong suspicions the "surveyor" is employed by a competing foreign company. Surveys may solicit proprietary information concerning corporate affiliations, market projections, pricing policies, program or technology director's names, purchasing practices, and types and dollar amounts of US Government contracts. An examination of the survey questions made evident the originator's actual intent was suspect.

Incidents involving the **co-opting of former employees** who had access to sensitive proprietary or classified S&T or program information remain a security concern. **Targeting cultural commonalities** to establish rapport is often associated with these incidents.

VI. Technology/MO Correlation

a. **Trends:** Unsolicited request for information (URFI) was the most frequently used foreign collection method in virtually all technology areas; however, there were no URFI pertaining to chemical and biological information. Similarly, twice as many marketing surveys as URFI pertained to militarily critical nuclear technologies. Using URFI to collect nuclear, biological, and chemical (NBC) data may be counterproductive. This is because a foreign entity may not know the questions to ask or the terminology to use to get needed scientific information. Foreign URFI specifying NBC information interest would arouse international suspicion concerning the intended use. This could indicate the direction of a foreign program, thus causing subsequent vulnerability to US NBC countermeasures. Requests for NBC data, prone to attract attention in the current international non-proliferation environment, i.e., chemical weapons convention, nuclear test ban, strategic arms reduction, etc., have a higher risk of interest detection.

Instead of URFI, foreign visits and possible exploitation of a joint venture were used as collection MO for chemical and biological information. Visits and joint ventures appear

less intrusive to US hosts and provide access with which foreign defense engineers, government-owned company employees, competitive company employees, and state academy scientists can probe and assess what is available for targeting and who may wittingly or unwittingly provide such data. In other words, a foreign representative can observe and, within reason, inquire without becoming suspicious. This demonstrates that certain MOs are more useful against certain targets.

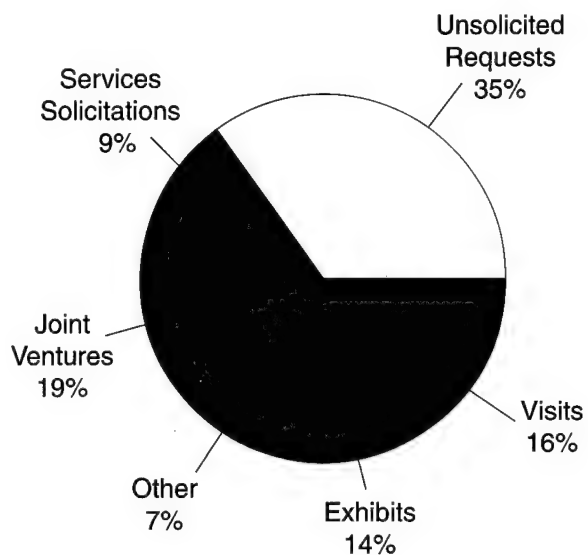
Electronics were also primarily targeted on foreign visits, joint ventures, and international conventions and seminars. This may be because written articles discuss theory and potential applications, but viewing an array, as it pertains to power output and electrical efficiency, may be more valuable to foreign interests. Many of the reports showed countries demonstrating patience and persistence in developing technology and technical information targets for collection at conventions, then later contacting the cleared employee, an associate, or a random addressee.

Other technologies where collection by viewing surpassed URFI included aeronautics, guidance and navigation, and space systems. Directed energy system technology was most often targeted at international conventions and exhibits. Guidance and navigation was most often targeted by solicitation and marketing of services.

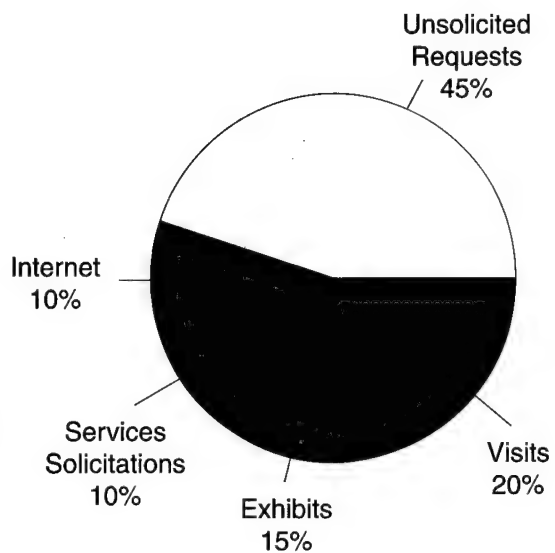
(Note: Identifying predominant MO for technologies is intended to prompt DSS/FSO discussion and SCM selection at cleared facilities developing these technologies.)

The following pie charts represent, for each technology, the prevalent MOs employed.

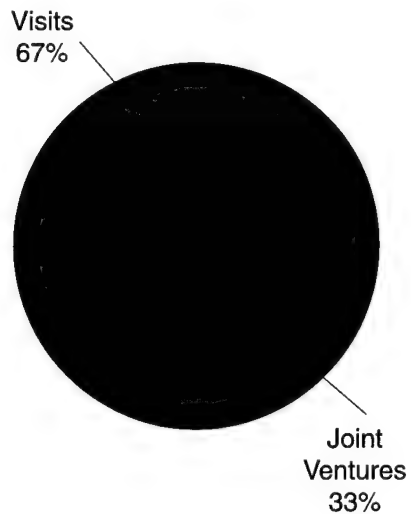
Aeronautic Systems Technology



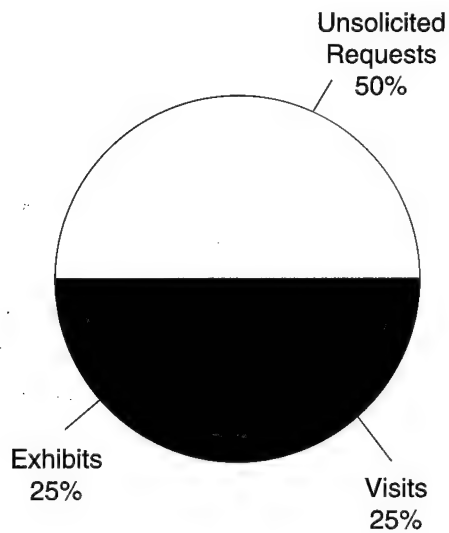
Armaments & Energetic Materials



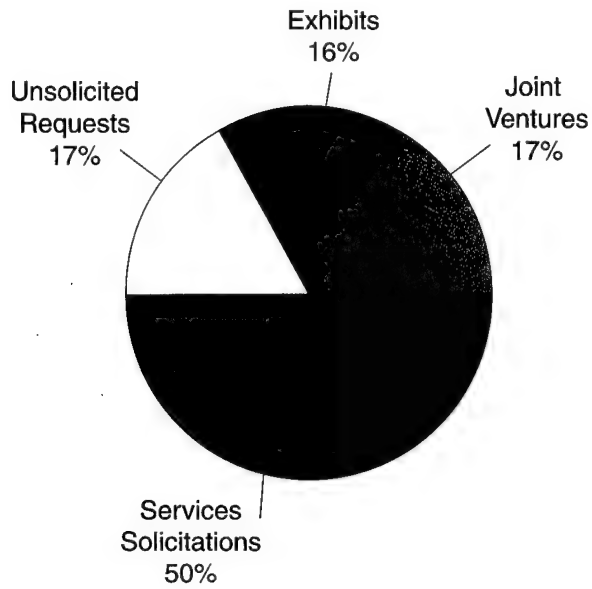
Chemical & Biological Systems



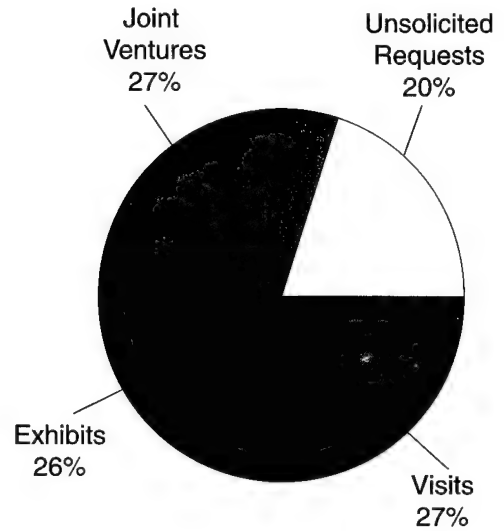
Directed & Kinetic Energy Systems



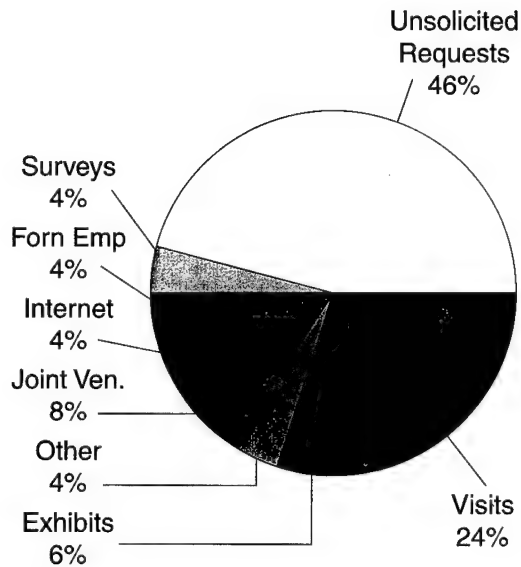
Guidance, Navigation, and Vehicle Control



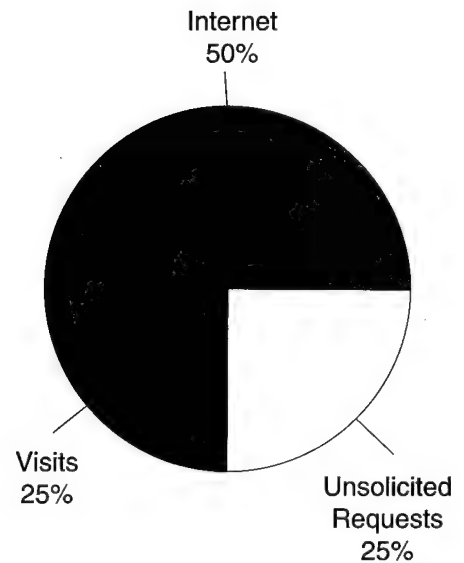
Electronics



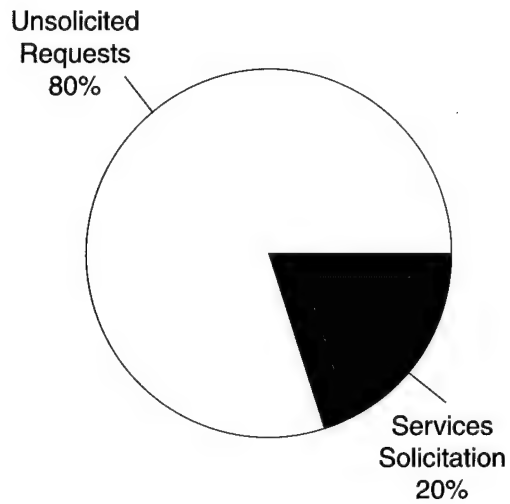
Information Systems



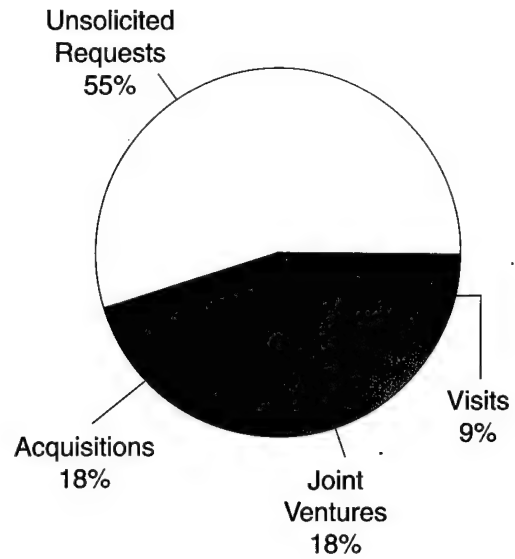
Information Warfare



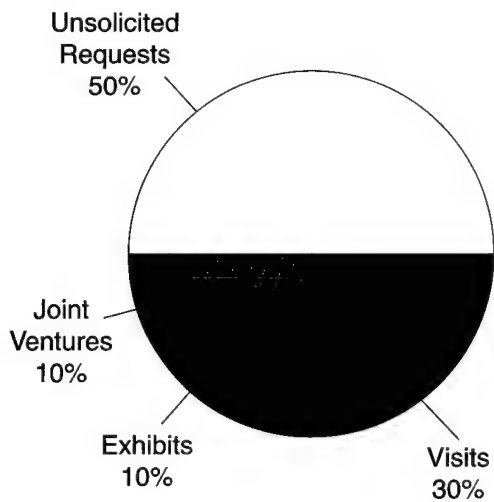
Manufacturing & Fabrication



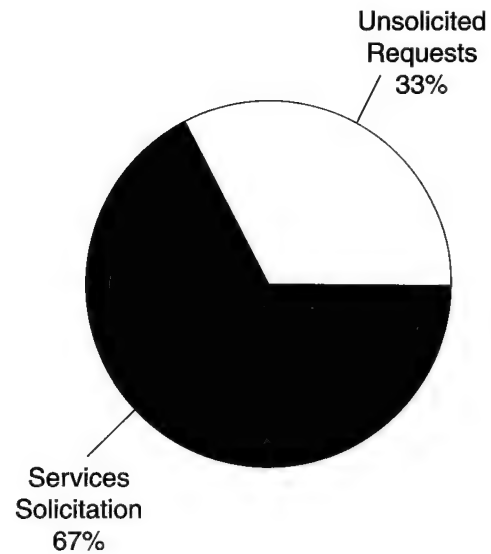
Marine Systems



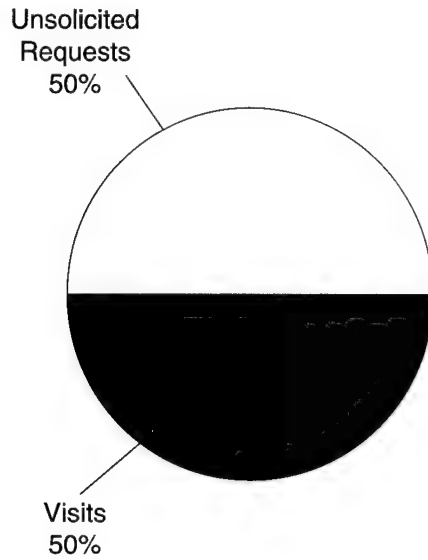
Materials



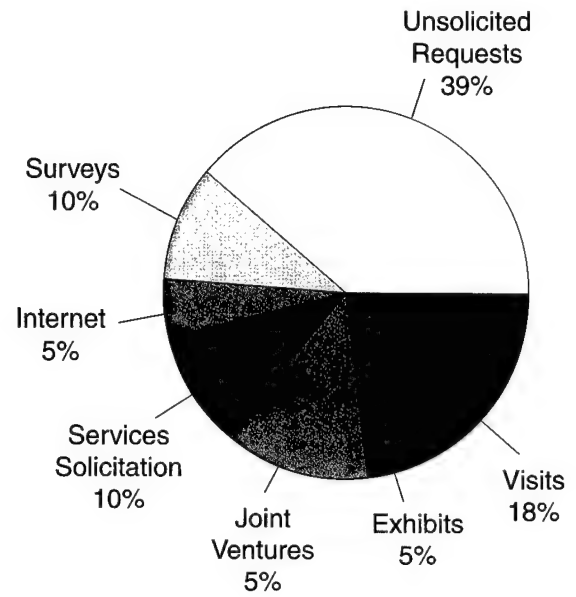
Nuclear Systems



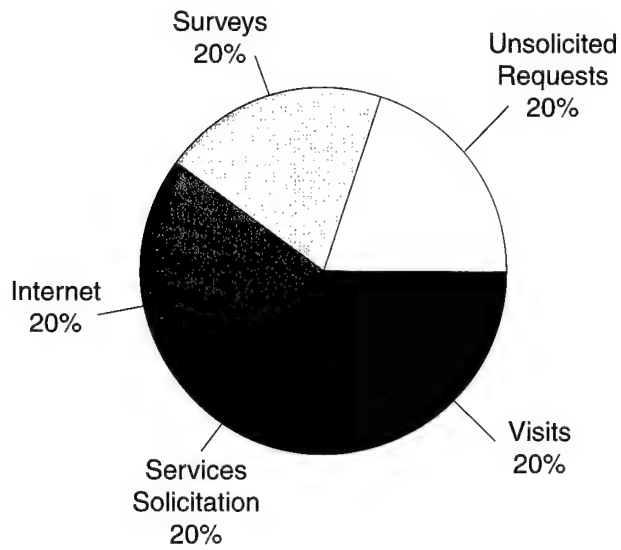
Power Systems



Sensors & Lasers



Signature Control



b. **Technical Intelligence Collection:** Airborne imagery often provides warning and description of *large* militarily critical objects (submarine in dry-dock, new fighter aircraft, new battle tank), but rarely can provide the critical program information: operational characteristics, survival vulnerability, efficient production/manufacturing process, and guidance algorithm. Viewing by human eyes can provide foreign interests with more details concerning operational capability and characteristics. People can see details that photos and images ignore. Seeing technology in research, development, engineering, testing, and evaluation scenes provides far more use than a photo; however, foreign interests still use imagery to target the US defense industry.

Foreign collectors employ signals intelligence (SIGINT) against priority targets. Monitoring telephonic communications helps countries assess how the militarily critical program is proceeding and when/where there may be a human intelligence (HUMINT) measurement, and signature (MASINT) or imagery intelligence (IMINT) collection opportunity, such as test-fire, unveiling ceremony, air show, or convention hosting cleared companies. Facsimile devices are intercepted by foreign entities with hopes of acquiring blueprints, system descriptions, design concepts, etc.

c. **Sequential Use of MOs:** DSS and cleared companies have recognized relationships between collection methods, but do not always report it. This is an important detail in determining the extent, intention, and next step of a foreign activity.

Sequential use of different methods is sometimes planned to limit risks and maximize collection efficiency. Other times, sequential MO indicate that one collection method failed. If a cleared company ignores URFI, a foreign entity may try another method. If a target is very important, foreign collectors may use several collection MOs in sequence or simultaneously. DSS reviews similar suspicious foreign activity across operating location boundaries to detect and identify foreign collection patterns of activity.

Several sequences appear more frequently and should still be clearly reported. After a cleared employee attends an international convention, his/her company is often contacted with an unsolicited request for information. Foreign visits often precede joint ventures because foreign entities want to insure that their goals can be achieved and their equities protected. Cleared companies should report commercial foreign visits if they identify a threat to their cleared employees or programs. DSS needs to help FSOs identify how threats to a defense program may originate from a foreign visitor or foreign employee conducting commercial, "dual-use", or joint research and development discussions.

The following matrix can be used to identify likely methods of operation (MOs) in order to enact threat appropriate security countermeasures. This matrix is based on 1997 cleared-company reporting of foreign interests employment of a MO versus a specified technology.

Technology Codes

- 1 = Aeronautics systems
- 2 = Armaments and energetic materials
- 3 = Chemical and biological systems
- 4 = Directed and kinetic energy systems
- 5 = Electronics
- 6 = Ground systems
- 7 = Guidance, navigation, and vehicle control
- 8 = Information systems
- 9 = Information warfare
- 10 = Manufacturing & fabrication
- 11 = Marine systems
- 12 = Materials
- 13 = Nuclear systems
- 14 = Power systems
- 15 = Sensors and lasers
- 16 = Signature control
- 17 = Space systems
- 18 = Weapons effects and countermeasures

MO Codes


- 1 =Unsolicited requests for S&T information
- 2 =Inappropriate conduct during visits
- 3 =Exploitation of joint ventures/research
- 4 =Targeting international exhibits, seminars, etc.
- 5 =Solicitation and marketing of services
- 6 =Marketing surveys
- 7 =Acquisitions of technology & companies
- 8 =INTERNET hacking/browsing
- 9 =Foreign employee collection
- 10 =Targeting former employees
- 11 =Targeting cultural commonalities


Use of the MO for particular technology is:

H = Highly likely

M = Likely

L = Least likely

 = Technology #6 - No reporting to assess

 = Technology #18 - Not enough reporting to assess

[illegible]

VII. Assessment of Future Trends

a. **Countries.** DSS forecasts that countries assessed most and moderately active from 1995-97 will continue technology collection operations against US defense industry. These foreign efforts will continue to be driven by military force modernization, economic competition, and commercial modernization using technologies with dual-use applications. Targeting dual-use technology affords foreigners the greatest yield considering the risk of US detection of diversion from stated end use.

b. **Targets.** In the Information Age, DSS expects increased foreign interest in electronics that are associated with information systems and information warfare. The recent increase in electronics collection seems to indicate the beginning of a surge in foreign interest. Electronics are key to providing faster, smarter, and better information solutions. The trend of acquiring technology that will inform decisionmakers, increase and speed information efficiency and flow, while simultaneously improving national and military capability, will remain consistent across tactical, operational, national, and strategic levels. For this reason, DSS expects the high levels of foreign interest and activity in the five most frequently reported MCTL categories to continue in 1998.

DSS assesses a resurgence in some MCTL categories that pertain to military superiority. In peace time, many developed countries are complacent with existing forces. Developing countries that never attained regional parity in combat power are assessed to become or remain interested in tried and tested US military technologies, such as those used in Operation Desert Storm. Advanced and developed countries are assessed to maintain or increase interest levels in enabling and enhancing technologies that modernize existing infrastructures (e.g. information security for government communications system) and major systems (e.g. weapons on UAVs or sensor-fused munitions). Newly realized, broader technology applications will also drive foreign collection efforts. For example, surface wave applications will increase foreign collection activity concerning acoustic technology.

DSS expects that developing countries will continue to seek advanced computing and communicating systems, while more advanced countries will target information system enhancements (MCTL foreign technology assessment demonstrates that nations' capabilities vary and this frequently parallels their level of collection activity.). Another premise for this forecast is that developed countries acquire information systems that facilitate inserting upgrades and enhancements. For example, developed countries prefer not to change computer systems each time they determine a need for software requiring additional

memory. DSS assesses countries whose targeting of computer and communications systems has waned will target enhancements and enabling technology in 1998.

c. **MOs.** DSS believes that foreign collection activities will increasingly use automated systems (e-mail and fax) to request information. Developing countries that do not use facsimiles may continue to solicit by mailed letters and post cards, while more-developed countries may transition from letter directly to e-mail. Fully-developed countries are using e-mail increasingly and we assess that trend to continue. Some developed country government, government-owned, and commercial entities routinely make maximum use of fax, letters, and e-mail. DSS often associates frequent or apparently automated post card requests with organized collection efforts from restricted countries. DSS is trying to determine which method of requests may indicate intelligence service, state-sponsored institute, government-owned company, or commercial enterprise involvement.

As the international political and economic environment continues to change and mature, US defense industry strategic management processes will be increasingly challenged to balance international marketing and partnerships with sound security countermeasures. Good risk management practices will ensure that cleared employees are properly trained and empowered to recognize and report suspicious activity.

If you believe that any of the above situations apply to your company, you should immediately notify your DSS Industrial Security Representative through your company Facility Security Officer. Likewise, notify DSS should you have any indication that your company or any of your employees may be the target of an attempted exploitation by the intelligence service of another country. **Reports of actual, probable, or possible espionage should be submitted to the FBI.**

This study was prepared by the Counterintelligence Office of the Defense Security Service based solely on reporting from the Defense Industrial Security Community.

The Defense Security Service greatly appreciates assistance from the National Counterintelligence Center in the design and publication of this report.

This brochure is approved
for public release.

OASD-PA/98-5-2028



